

What Is Claimed Is:

- 1 1. A method to facilitate locking an adversary out of a network
2 application, comprising:
3 receiving at a server a request, including an authentication credential, to
4 access the network application, wherein the authentication credential includes a
5 user identifier associated with a user and a network address of a user device;
6 examining an audit log to determine if the user identifier has been locked
7 out from the network address; and
8 if the user identifier has been locked out from the network address,
9 denying access to the network application;
10 otherwise, checking the authentication credential for validity, and
11 if the authentication credential is valid,
12 allowing access to the network application,
13 otherwise,
14 logging a failed attempt in the audit log, wherein the
15 user identifier is locked out from the network address after
16 a threshold number of failed attempts, and
17 denying access to the network application;
18 whereby the adversary is prevented from accomplishing an attack by
19 masquerading as the user.
- 1 2. The method of claim 1, further comprising imposing a global
2 lockout for the user identifier after a threshold number of network addresses are
3 locked out for the user identifier.

1 3. The method of claim 2, further comprising removing a lockout
2 after a predetermined period of time.

1 4. The method of claim 2, further comprising manually removing a
2 lockout by an administrator of the server.

1 5. The method of claim 1, wherein the authentication credential
2 includes a user name and a password.

1 6. The method of claim 5, wherein checking the authentication
2 credential for validity involves:
3 verifying that an administrator has authorized access to the network
4 application for a combination of the user name and the password; and
5 determining if the request violates an access rule in a rule table.

1 7. The method of claim 6, wherein the access rule can specify:
2 an allowed time-of-day;
3 an allowed number of access attempts;
4 an allowed network address; and
5 an allowed network domain.

1 8. The method of claim 1, wherein the network address includes an
2 Internet Protocol address.

1 9. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method to
3 facilitate locking an adversary out of a network application, comprising:

4 receiving at a server a request, including an authentication credential, to
5 access the network application, wherein the authentication credential includes a
6 user identifier associated with a user and a network address of a user device;
7 examining an audit log to determine if the user identifier has been locked
8 out from the network address; and
9 if the user identifier has been locked out from the network address,
10 denying access to the network application;
11 otherwise, checking the authentication credential for validity, and
12 if the authentication credential is valid,
13 allowing access to the network application,
14 otherwise,
15 logging a failed attempt in the audit log, wherein the
16 user identifier is locked out from the network address after
17 a threshold number of failed attempts, and
18 denying access to the network application;
19 whereby the adversary is prevented from accomplishing an attack by
20 masquerading as the user.

1 10. The computer-readable storage medium of claim 9, the method
2 further comprising imposing a global lockout for the user identifier after a
3 threshold number of network addresses are locked out for the user identifier.

1 11. The computer-readable storage medium of claim 10, the method
2 further comprising removing a lockout after a predetermined period of time.

1 12. The computer-readable storage medium of claim 10, the method
2 further comprising manually removing a lockout by an administrator of the server.

1 13. The computer-readable storage medium of claim 9, wherein the
2 authentication credential includes a user name and a password.

1 14. The computer-readable storage medium of claim 13, wherein
2 checking the authentication credential for validity involves:
3 verifying that an administrator has authorized access to the network
4 application for a combination of the user name and the password; and
5 determining if the request violates an access rule in a rule table.

1 15. The computer-readable storage medium of claim 14, wherein the
2 access rule can specify:
3 an allowed time-of-day;
4 an allowed number of access attempts;
5 an allowed network address; and
6 an allowed network domain.

1 16. The computer-readable storage medium of claim 9, wherein the
2 network address includes an Internet Protocol address.

1 17. An apparatus to facilitate locking an adversary out of a network
2 application, comprising:
3 a receiving mechanism that is configured to receive at a server a request,
4 including an authentication credential, to access the network application, wherein
5 the authentication credential includes a user identifier associated with a user and a
6 network address of a user device;

7 an examining mechanism that is configured to examine an audit log to
8 determine if the user identifier has been locked out from the network address; and
9 an access mechanism that is configured to deny access to the user
10 identifier if the user identifier has been locked out from the network address;
11 a validation mechanism that is configured to check the authentication
12 credential for validity, wherein the access mechanism is further configured to
13 allow access if the authentication credential is valid; and
14 a logging mechanism that is configured to log a failed attempt in the audit
15 log, wherein the user identifier is locked out from the network address after a
16 threshold number of failed attempts, and wherein the access mechanism is further
17 configured to deny access to the user identifier after a failed access attempt;
18 whereby the adversary is prevented from accomplishing an attack by
19 masquerading as the user.

1 18. The apparatus of claim 17, further comprising a lockout
2 mechanism that is configured to impose a global lockout for the user identifier
3 after a threshold number of network addresses are locked out for the user
4 identifier.

1 19. The apparatus of claim 18, further comprising a lockout removing
2 mechanism that is configured to remove a lockout after a predetermined period of
3 time.

1 20. The apparatus of claim 18, further comprising a lockout removing
2 mechanism that is configured to allow an administrator of the server to manually
3 remove a lockout.

1 21. The apparatus of claim 17, wherein the authentication credential
2 includes a user name and a password.

1 22. The apparatus of claim 21, further comprising:
2 a verification mechanism that is configured to verify that an administrator
3 has authorized access to the network application for a combination of the user
4 name and the password; and
5 a violation determining mechanism that is configured to determine if the
6 request violates an access rule in a rule table.

1 23. The apparatus of claim 22, wherein the access rule can specify:
2 an allowed time-of-day;
3 an allowed number of access attempts;
4 an allowed network address; and
5 an allowed network domain.

1 24. The apparatus of claim 17, wherein the network address includes
2 an Internet Protocol address.